

【媒體報導】蓋亞資訊攜手一零四資訊展現Chronicle效能，瞄準自動化資安之路前行

(原文出處：[蓋亞資訊攜手一零四資訊展現Chronicle效能，瞄準自動化資安之路前行@數位時代](#))

104科技攜手蓋亞資訊，善用Google Chronicle解決方案快速部署、高度競爭力價格與強大功能等特性，打造高效資安平台保護上百萬會員個資。



管控資訊安全威脅與風險是企業面對動盪時代下所不可或缺的營運策略，由於面對日誌(Log)種類眾多與數量龐大的紀錄，對資安團隊普遍存在警示疲勞與難以消化的窘境，非但影響面對威脅的決策品質，尤有甚者，目前所見的趨勢中，發現駭客入侵後可能潛伏在企業內的電腦系統中長達十天甚至上百天，所以企業應對此一挑戰，善用資安平台內的Log訊息與回溯查詢的功能，就變成最佳資安執行策略的基礎。

Google的Chronicle雲原生解決方案以隨時可以查詢365天的日誌資訊，搭配高效SIEM(Security Information and Event Management)平台，提供企業嶄新的使用典範，以完整且清晰的戰略視角，協助企業因應層出不窮且千變萬化的資安事件，以縮小損害範圍。透過一零四資訊科技(簡稱104)資深資安經理林尚達先生，與蓋亞資訊執行長吳炳鈞先生以下的問答，展現雙方合作所創造的商業成功的契機。



▲一零四資訊科技資深資安經理林尚達認為：Google的Chronicle雲原生解決方案以快速與容易佈署、具備高度價格競爭性與強大的功能而被104認可與勝出。

請問104科技如何透過SIEM解決方案打造一個值得信賴的求職、求才的雲端服務？

林尚達答：104科技擁有數百萬會員與使用者資訊，其中，個人履歷內容包含大量個人資料與高敏感性的訊息，是駭客長期鎖定的攻擊目標，因此重視資安與個資保護是104營運的關鍵訴求之一。目前除了持續關注外部威脅的動態情報與新世代資安防護解決方案之外，並參考國際資安防護框架與國家公佈之資安規範指引，建立內部資安組織與應變團隊，藉由多層次縱深的資安防禦系統，預防個資外洩的發生。

104持續用最嚴格的資安標準來檢視所提供的各項產品服務，以104「企業大師」雲端人資管理系統為例，該系統提供多元化出勤打卡、人事表單審核、薪資自動結算到排班管理等功能，幫助中小企業提高人資管理效率、減輕人事作業上的繁瑣、增加團隊協作溝通的解決方案，讓中小企業也可以擁有大企業人力資源管理的強大功能。系統所儲存各項機敏資訊如員工個人資料及薪資等更是重點保護對象，資料內容的儲存與傳遞採用加密機制，開發須符合安全軟體開發生命週期，上線前通過各項安全檢測，旨在提供最安全的人資管理平台服務。

由於104各項產品服務的伺服器、DNS、防火牆、Windows主機等端系統日誌，以及O365、EDR等雲端日誌，大量記錄著每一筆連線與處理動作，Log資料量相當驚人，若是用傳統商用的SIEM解決方案，由於計價以儲存容量為主的模式，想要儲存一年期的資料，往往所費不貲；而Open Source解決方案卻容易卡在資料規模過於龐大與複雜，運算資源需求爆增，以及操作不易，使得系統變得難以滿足企業對於資安監控的需求，甚至遇到服務品質不穩定或日誌數據丟失等慘劇，而Google的Chronicle雲原生解決方案以快速與容易佈署、具備高度競爭力價格與強大的功能而被104認可與勝出。



▲蓋亞資訊執行長吳炳鈞表示：Chronicle可以往後端延伸到Google Cloud旗下的Looker及BigQuery所提供的資料分析與可視化的整合作業，提供企業最佳的商業智慧(BI)解決方案。

請問蓋亞資訊如何看Google的Chronicle雲端服務的優勢？

吳炳鈞答：蓋亞資訊多年在企業資安與雲端維運服務的第一手經驗，對於衡量104所需要打造的雲端服務電商平台的需求，大力推薦使用Chronicle解決方案，首先其所需要投入的軟體授權及硬體成本，是最物超所值的選擇，以目前台灣市場上知名品牌的SIEM及Logger平台的性價比的優勢來觀察，Google Chronicle最具競爭性，蓋亞資訊同時也是台灣正式代理資格的廠商之一。Chronicle能兼顧收集、分析日常資安的Log，具備資安趨勢洞察能力，以協助企業客戶預防未來發生的風險與威脅。

Google Cloud最大的優勢就是提供企業快速佈署的優勢，善用龐大的雲端儲存容量與運算處理的速度，擺脫儲存容量大小的箝制，而改用員工數量來做版權的計價基礎，讓企業得以清楚掌握親民的成本結構，並僅需幾小時便可以迅速啟用整個系統，另外Chronicle可以處理Petabyte等級的雲端儲存空間，以及快速的資料搜尋的技術，而且可以將同樣的資料往後端延伸到Google Cloud旗下的Looker及BigQuery所提供的資料分析與可視化的整合作業，提供企業最佳的商業智慧(BI)解決方案，整體架構一氣呵成，無須額外花費資料移轉、複製等使用，簡化實際運作的難題。



▲104科技利用Chronicle除了製作Dashboard等顯示看板以方便於日常營運，而調查分析作業可從數小時縮短為數分鐘內完成，效益令人滿意。

請問104科技如何使用Chronicle解決方案在企業內發揮最大的使用效益與價值？

林尚達答：104利用Chronicle製作Dashboard等顯示看板的資訊，以做為日常資安維運作業的監控，尤其針對大量的資安告警，無論是國際資安業者、TWCERT所發佈的重大資安事件等情資，調查分析作業可從數小時縮短為數分鐘內完成，做到快速確認公司內資安威脅軌跡的追蹤，並及時啟動資安應變程序。



▲蓋亞資訊陳瑞璋業務經理與104科技資深資安經理林尚達期雙方合作可以更上一层楼。

請問蓋亞資訊如何攜手104科技塑造Chronicle解決方案的成功範例？

吳炳鈞答：觀察Chronicle系統在104內部的使用典範中，發現他們已經把使用的範疇延伸到網管維運與軟體產品開發團隊的使用，並規劃未來透過Chronicle所提供API介面，同步整合與串接SOAR等自動化應用，透過「標準化」工作流程及「自動化」腳本，加速企業內部資安事件通報與應變管理流程，提升資安團隊作業效率及生產力，這都有賴於蓋亞資訊所提供7x24技術支援與諮詢服務，尤其扮演與Google Cloud技術服務團隊的整合與溝通的關鍵，讓Chronicle快速在104資安與網管團隊發揮重要的效益。

GCP Premier Partner | 蓋亞資訊

蓋亞資訊為台灣GCP Premier Partner，是台灣許多大企業指名使用的雲端服務，提供擴充性極高的儲存空間以及高效能的執行速度，滿足所有產業的需求，GCP具有前瞻性的基礎架構，長期使用也不會被時間淘汰；且功能強大的資料與分析服務，打造出更優質的產品；數據中心設立於台灣彰濱，提供台灣本土用戶最優的連線品質。

蓋亞資訊是GCP官方認證的青英合作夥伴，並成為台灣第一家取得GCP Chronicle Reseller資格的合夥夥伴，擁有超過百張認證的專業工程師團隊，提供7x24全年無休的維運服務，隨時解決企業問題。蓋亞資訊已服務超過八百家客戶，擁有豐富的雲端及資安經驗，服務範圍橫跨台灣、大陸、香港、菲律賓、東南亞其他地區及歐美，企業類型包含製造業、金融業、航運業、遊戲業、媒體娛樂業等等，可為企業提供量身訂做的顧問服務。

